

REMARKS

Claims 1-3 and 5-29 are pending in this application. By this Amendment, claims 1, 5, 6, 8-10, 12 and 13 are amended, claim 4 is canceled, and new claims 14-29 are added.

In particular, claims 1, 12 and 13 are amended to incorporate features originally recited in claim 4, and some features originally recited in claim 5. Accordingly, claim 4 is canceled, and claim 5 is appropriately amended. In addition, claims 5, 6, 8-10, 12 and 13 are also amended to improve their wording. No new matter is added.

Reconsideration of the application is respectfully requested.

Applicant thanks Examiners Morse and Smithers for the courtesy extended to Applicant's representative, Mr. Luo, during the November 13, 2003, personal interview. The substance of the personal interview is incorporated in the following remarks.

The Office Action rejects claims 5-11 under 35 U.S.C. §112, second paragraph. This rejection is respectfully traversed.

The Office Action asserts that Fig. 1 indicates that the depositaries reside on the server, Applicant respectfully submits that Fig. 1 is not limited to such an indication. In particular, as discussed during the November 13, 2003, personal interview, item 102 of Fig. 1 includes "depositary selection rules," and "deposited private key list." There is no indication in Fig. 1 that item 102 must include depositaries.

For at least the above reasons, withdrawal of the rejection of claims 5-11 under 35 U.S.C. §102, second paragraph, is respectfully requested.

The Office Action rejects claims 1-4, 12 and 13 under 35 U.S.C. §102(b) over U.S. Patent 5,436,972 to Fischer. This rejection is respectfully traversed.

The Office Action asserts that Fischer discloses all elements recited in claims 1-4, 12 and 13. Applicant respectfully submits that Fischer does not disclose or suggest a server that, in response to a recovery request from the depositary, sends to said depositary said recovery

information encrypted by said public key of said depositary, and acquires from said depositary said recovery information decrypted by a private key of said depositary and then encrypted by a public key of said server, as recited in claims 1-4, and similarly recited in claims 12 and 13.

As discussed during the November 13, 2003 personal interview, Fischer discloses an escrowed secret information retrieval scheme in which a trustee evaluates a retrieval request from an applicant. See col. 10, lines 49-54. The applicant is required to submit an escrow information record 80 and documentation containing credentials which can be used to verify that the applicant is the legitimate owner of the secret information. See col. 10, lines 54-63. The escrow information record 80 has already been created and encrypted in a definition phase prior to the retrieval phase. See col. 9, lines 8-11, and col. 10, lines 24-27. The escrow information record 80 is not created or encrypted during the retrieval phase.

As discussed during the November 13, 2003 personal interview, the documentation contains credentials such as an affidavit executed by a notary public attesting to the applicant's characteristics. See col. 10, lines 60-66. This documentation is not encrypted, but is to be compared with standard escrow information submitted in the definition phase. See Fig. 2 and col. 7, lines 7-34. Fischer does not disclose or suggest acquiring recovery information decrypted by a private key of the requestor and then encrypted by a public key in response to a recovery request. Therefore, Fischer does not disclose or suggest a server that, in response to a recovery request from the depositary, sends to said depositary said recovery information encrypted by said public key of said depositary, and acquires from said depositary said recovery information decrypted by a private key of said depositary and then encrypted by a public key of said server, as recited in claims 1-4. Nor does Fischer teach or disclose the generally similar features recited in claims 12 and 13.

For at least the above reasons, Fischer does not disclose or suggest all elements recited in claims 1-4, 12 and 13. Thus, Fischer does not disclose or suggest the subject matter recited in

claims 1-4, 12 and 13. Withdrawal of the rejection of claims 1-4, 12 and 13 under 35 U.S.C. §102(b) is respectfully requested.

New claims 14-29 are patentable for at least the reasons set forth above that are relevant to their features.

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claims 1-3 and 5-29 are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in better condition for allowance, the Examiner is invited to contact Applicant's undersigned representative at the telephone number listed below.

Respectfully submitted,



James A. Oliff
Registration No. 27,075

Gang Luo
Registration No. 50,559

JAO:GXL/sqb

Date: December 29, 2003

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION Please grant any extension necessary for entry; Charge any fee due to our Deposit Account No. 15-0461
--